UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,212	01/29/2002	Robert J. Lambert	00001-0420	2200

27871 7590 09/16/2005

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER
ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/058,212	**Applicant(s)** LAMBERT, ROBERT J.	
	Examiner Kaveh Abrishamkar	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on January 29, 2002. Claims 1-6 were originally received for consideration. No preliminary amendments for the claims were received. Claims 1-6 are currently being considered.

Claim Objections

2. Claims 4 and 6 are objected to because of the following informalities: Both claims are not concluded with a period, but instead, are concluded with a semicolon. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1 recites the limitation "said predetermined number of machine words" in limitation a) of the claims. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone (U.S. Publication No. US 2002/0136402 A1).

Regarding claim 1, Vanstone discloses:

A method of adding elements of a finite field F.sub.2.sub..sup.m, where m is less than a predetermined number n, said method comprising the steps of:

a) storing a first and a second element in a pair of registers, each of said pair of registers comprising said predetermined number of machine words (paragraphs 16,20,40,42);

b) establishing an accumulator having said predetermined number of machine words (paragraphs 13,19-21,48);

c) computing for each of said machine words in said accumulator the exclusive-or of the corresponding machine words representing each of said first and second elements (paragraphs 46,57,59-61).

Regarding claim 2, Vanstone discloses:

A device for adding a pair of elements of a finite field F.sub.2.sub..sup.m where m is less than a predetermined number n, comprising:

a) a pair of registers for storing said pair of elements, each of said registers consisting of n machine words (paragraphs 16,20,40,42);

b) an accumulator consisting of n machine words (paragraphs 13,19-21,48);

c) an output register consisting of n machine words (paragraphs 16,20,40,42);

d) an XOR gate connected to a respective machine word in each of said pair of registers and providing an output to a respective one of said machine words (paragraphs 46,57,59-61).

Regarding claim 3, Vanstone discloses:

A finite field multiplier operable to multiply two elements of one of a plurality of finite fields, said finite fields being partitioned into subsets, said multiplier comprising:

a) a plurality of wordsized finite field multipliers, each suitable for multiplying elements of each finite field in a respective subset of said plurality of finite fields (paragraphs 50,56);

b) a finite field reducer configured to perform reduction in said one finite field (paragraphs 41,43,50);

c) a processor (paragraphs 17,43) configured to

i) operate the wordsized finite field multiplier suitable for use with said one finite field to obtain an intermediate product (paragraphs 55-56); and

ii) operate said finite field reducer on said intermediate product to obtain the product of the two elements (paragraphs 41,43,55).

Regarding claim 4, Vanstone discloses:

A method of performing a finite field operation on two elements r, s of a finite field, comprising the steps of:

a) performing a wordsized operation of r and s, said wordsized operation corresponding to said finite field operation (paragraphs 50,55-56);

b) performing a modular reduction of the result of step a) (paragraph 55).

Regarding claim 5, Vanstone discloses:

A finite field engine for performing a finite field operation on at least one element of a finite field chosen from a set of finite fields, said set of finite fields being divided into subsets according to their word size, comprising:

a) a finite field operator for each of said subsets (paragraphs 50,55-56);

b) a finite field reducer for each of said finite fields (paragraphs 41,43,55);

c) a processor (paragraphs 17,43) configured to choose the finite field operator corresponding to the subset containing said chosen finite field and the finite field reducer for said chosen finite field and apply the chosen finite field operator to said element to produce an intermediate result and apply the chosen finite field reducer to said intermediate result to obtain the result of said finite field operation (paragraphs 50,55-56).

Regarding claim 6, Vanstone discloses:

A cryptographic system comprising:

a) a plurality of elliptic curves, each specifying elliptic curve parameters and a respective finite field (paragraphs 43), wherein the plurality of elliptic curves correspond to the different sized fields;

b) a plurality of finite field settings corresponding to each finite field (paragraph 43), wherein the finite fields can be of different sizes;

c) a plurality of wordsized finite fields, each having routines, each finite field being assigned to one of said wordsized finite fields (paragraph 43), wherein the finite fields can be of different sizes;

d) a reduction routine for each finite field (paragraph 41,43, 55);

e) a computational apparatus configured to perform a cryptographic operation by the steps of:

i) selecting one of said elliptic curves (paragraphs 18-22);

ii) performing a cryptographic function using the routines from the wordsized finite field to which the respective finite field corresponding to said selected elliptic curve is assigned (paragraphs 50,55-56).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

KA
09/13/2005